ORIGINAL

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means ❒ Original ❒ Duplicate Original

UNITED STATES DISTRICT COURT

for the

District of Oregon

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* The person of John Middendorp and the premises located at 11575 SW Greenburg Road Apt. 12, Tigard, OR 97223, more fully described in Attachment A	)	Case No. 3:22-mc-00247

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the _____ District of Oregon
(identify the person or describe the property to be searched and give its location):

The person of John Middendorp and the premises located at 11575 SW Greenburg Road Apt. 12, Tigard, OR 97223, more fully described in Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

The information and items set forth in Attachment B hereto.

YOU ARE COMMANDED to execute this warrant on or before 3/22/2022 *(not to exceed 14 days)*
☑ in the daytime 6:00 a.m. to 10:00 p.m. ❒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Honorable Stacie F. Beckerman, via the Clerk .
(United States Magistrate Judge)

❒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*
❒ for _____ days *(not to exceed 30)* ❒ until, the facts justifying, the later specific date of _____ .

Date and time issued: 3/8/2022 8:12 p.m.

Stacie F. Beckerman
Judge's signature

City and state: Portland, Oregon Honorable Stacie F. Beckerman, U.S. Magistrate Judge
Printed name and title

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means (Page 2)

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
3:22-mc-00247	March 9, 2022 @ 2:00 p.m.	John Middendorp / Paul Hartline

Inventory made in the presence of : SA Clinton Lindsly / SA Justin Moshofsky

Inventory of the property taken and name(s) of any person(s) seized:

Samsung Galaxy A13 5G S/N R5CT118J3YE - 971-707-6413

Samsung Chromebook Tablet S/N 4WQR9FFR309424A

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: March 13, 2022

CLINTON B LINDSLY

Digitally signed by CLINTON B LINDSLY
Date: 2022.03.13 08:57:07 -07'00'

Executing officer's signature

Clinton Lindsly , HSI Special Agent

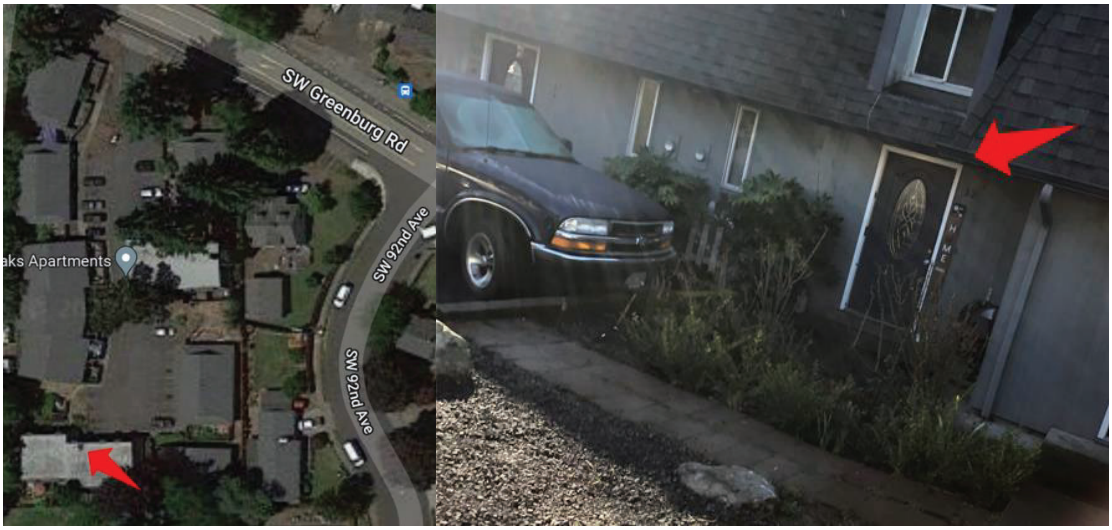
Printed name and title

ATTACHMENT A

Description of the Premises, Property, and Person to be Searched

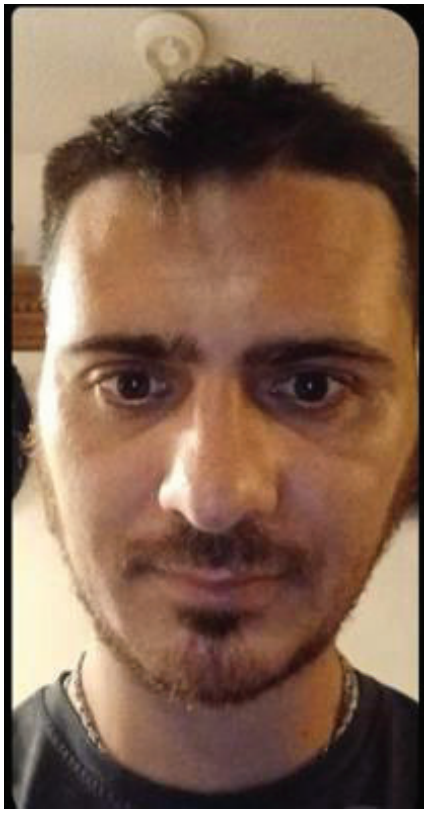
1. Subject Premises: 11575 SW Greenburg Road Apt. 12, Tigard, OR 97223

The Subject Premises is an apartment or duplex located at 11575 SW Greenburg Road Apt. 12, Tigard, OR 97223. It is a wood two-story residence painted blue, with a black roof, faces north, and is located on the south side of SW Greenburg Road. The number "12" is on the west side of the front door in black lettering. Specifically, common areas of the residence, any room rented, controlled, or used by **John MIDDENDORP**, and any area in which his belongings are reasonably believed to be stored.



2. Person

The person of **John MIDDENDORP** (and any cell phone or digital device on his person or under his control at the time of search, provided that he is located in the District of Oregon at the time of search), with date of birth XX/XX/1989; California Identification #E2189680; a white male with black hair; approximately 5'11"; and 155 lbs., pictured below.



ATTACHMENT B

Items to be Searched For, Seized, and Examined

The following items, documents, and records that contain contraband or are evidence, fruits, or instrumentalities of violations of 18 U.S. Code § 2250(a) (Failure to Register as a Sex Offender), 18 U.S.C. §§ 2251(a) and (e) (Attempted Sexual Exploitation of a Child), and 18 U.S.C. § 1470 (Attempted Transfer of Obscene Material to a Minor), collectively referred to as the "**Target Offenses**," including the following:

I. Digital Evidence

1. Any mobile devices including cell phones that may have been used to commit or facilitate the **Target Offenses**;

2. Any computers that may have been used to facilitate violations of the **Target Offenses**, including any peripheral devices such as external hard drives, external disk drives, power supplies, modem, and routers;

3. Any computer equipment or digital devices that are capable of being used to create, access, or store contraband or evidence, fruits, or instrumentalities of the **Target Offenses**, including central processing units; laptop or notebook computers; personal digital assistants; wireless communication devices including paging devices and cellular telephones; peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communication devices such as modems, routers, cables, and connections; storage media; and security devices;

4. Any magnetic, electronic, or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD ROMs, CD-Rs, CD-RWs, DVDs, optical disks, printer or memory buffers, thumb drives, smart cards, PC cards, memory calculators, electronic dialers,

electronic notebooks, personal digital assistants, and cell phones capable of being used to commit or further the crimes referenced above, or to create, access, or store contraband, or evidence, fruits, or instrumentalities of such crimes;

5. Any documentation, operating logs, and reference manuals regarding the operation of the computer equipment, storage devices, or software;

6. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;

7. Any physical keys, encryption devices, dongles, or similar physical items which are necessary to gain access to the computer equipment, storage devices, or data;

8. Any passwords, password files, test keys, encryption codes, or other information necessary to access the computer equipment, digital devices, storage devices, cloud-based storage accounts, or data; and

9. All records, documents, programs, applications, or materials created, modified, or stored in any form, including in digital form, on any computer or digital device, that show the actual user(s) of the computers or digital devices during the time the device was used to commit the crimes referenced above, including the web browser's history; temporary Internet files; cookies, bookmarked, or favorite web pages; email addresses used from the computer; MAC IDs and/or Internet Protocol addresses used by the computer; email, instant messages, and other electronic communications; address books; contact lists; records of social networking and online service usage; screen names or usernames, and software that would allow others to control the digital device such as viruses, Trojan horses, and other forms of malicious software.

II. Records, Documents, and Visual Depictions

10. Any records, documents, or materials, including correspondence, that pertain to any travel of **MIDDENDORP** from December 24, 2021 (date of end of supervision in California) to the present;

11. Any records, documents, or materials, including correspondence, that pertain to any communications in any form with the online "persona," including on Facebook;

12. Any photographs, videos, or recordings of HSI Special Agent Erin Herrgott;

13. Any photographs, videos, or recordings of **MIDDENDORP** that appear sexual in nature consistent with what he sent the undercover persona;

14. Any records, documents, or materials, including encryption codes, encryption links, or passcodes related to the any account used or believed to have been used to communicate with the undercover persona described in the affidavit in support of the search warrant application;

15. Any records, documents, or materials, including any record related to the creation of or any correspondence to or from any Facebook account identified in the affidavit in support of the search warrant application in any form;

16. Any records, documents, or materials, including any correspondence, that involve any communication with any person who is or appears to be under the age of 18, that are sexual in nature, that discuss the production or transmission of sexually explicit images of a minor, or indicate a sexual interest in children;

17. Any records, documents, or materials, including correspondence, that pertain to the production, transportation, distribution, receipt, or possession of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

18. Any records, documents, or materials which include offers to transmit, through interstate commerce by any means (including by computer), any visual depiction of a minor engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

19. Any records, documents, or materials relating to the production, reproduction, receipt, shipment, trade, purchase, or a transaction of any kind involving the transmission, through interstate commerce (including by computer), of any visual depiction of a minor engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

20. Any records, documents, or materials naming or identifying minors visually depicted while engaging in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

21. Any records of Internet usage, including records containing screen names, usernames, and e-mail addresses, and identities assumed for the purposes of communication on the Internet. These records include billing and subscriber records, chat room logs, e-mail messages, and include electronic files in a computer and on other data storage media, including CDs or DVDs;

22. Any records, documents, or materials referring or pertaining to communications with others, whether in person, by telephone, or online, for the purpose of producing, distributing, or transporting child pornography, including chat logs, call logs, address book or contact list entries, and digital images or videos sent or received; and

As used above, the terms records, documents, programs, applications or materials includes records, documents, programs, applications or materials created, modified or stored in any form including digital or electronic form.

Search Procedure

26. In searching for data capable of being read, stored, or interpreted by a computer or storage device, law enforcement personnel executing the search warrant will employ the following procedure:

a. *On-site search, if practicable.* Law enforcement officers trained in computer forensics (hereafter, "computer personnel"), if present, may be able to determine if digital devices can be searched on site in a reasonable amount of time without jeopardizing the ability to preserve data on the devices. Any device searched on site will be seized only if it contains data falling within the list of items to be seized as set forth in the warrant and herein.

b. *On-site imaging, if practicable.* If a digital device cannot be searched on site as described above, the computer personnel, if present, will determine whether the device can be imaged on site in a reasonable amount of time without jeopardizing the ability to preserve the data.

c. *Seizure of digital devices for off-site imaging and search.* If no computer personnel are present at the execution of the search warrant, or if they determine that a digital device cannot be searched or imaged on site in a reasonable amount of time and without jeopardizing the ability to preserve data, the digital device will be seized and transported to an appropriate law enforcement laboratory for review.

d. Law enforcement personnel will examine the digital device to extract and seize any data that falls within the list of items to be seized as set forth in the warrant and herein. To the extent they discover data that falls outside the scope of the warrant that they believe should be seized (e.g., contraband or evidence of other crimes), they will seek an additional warrant.

e. Law enforcement personnel will use procedures designed to identify items to be seized under the warrant. These procedures may include the use of a "hash value" library to

exclude normal operating system files that do not need to be searched. In addition, law enforcement personnel may search for and attempt to recover deleted, hidden, or encrypted data to determine whether the data falls within the list of items to be seized under the warrant.

f. If the digital device was seized or imaged, law enforcement personnel will perform an initial search of the original digital device or image within a reasonable amount of time not to exceed 120 days from the date the warrant is executed. If, after conducting the initial search, law enforcement personnel determine that an original digital device contains any data falling within the list of items to be seized pursuant to this warrant, the government will retain the original digital device to, among other things, litigate the admissibility/authenticity of the seized items at trial, ensure the integrity of the copies, ensure the adequacy of chain of custody, and resolve any issues regarding contamination of the evidence. If the government needs additional time to determine whether an original digital device or image contains any data falling within the list of items to be seized pursuant to this warrant, it may seek an extension of time from the Court within the original 120-day period from the date the warrant is executed. The government shall complete the search of the digital device or image within 180 days of the date the warrant is executed. If the government needs additional time to complete the search, it may seek an extension from the Court.

g. If, at the conclusion of the search, law enforcement personnel determine that particular files or file folders on an original digital device or image do not contain any data falling within the list of items to be seized pursuant to the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the list of items to be seized pursuant to the warrant, as well as data within the operating system, file system, or software application relating or pertaining

to files or data falling within the list of items to be seized pursuant to the warrant (such as log files, registry data, and the like), through the conclusion of the case.

h. If an original digital device does not contain any data falling within the list of items to be seized pursuant to this warrant, the government will return that original data device to its owner within a reasonable period of time following the search of that original data device and will seal any image of the device, absent further authorization from the Court.